

文章编号: 1006-2467(2024)10-1596-10

DOI: 10.16183/j.cnki.jsjtu.2023.151

三角形结合方案的最优局部修复码构造

王 静, 李静辉, 杨佳蓉, 王 娥

(长安大学 信息工程学院, 西安 710018)

摘 要: 局部修复码(LRCs)为用于分布式存储系统中的新型纠删码,能够有效实现海量数据的可靠高效存储,构造具有 (r, t) 局部性的 LRCs 已成为当前研究热点.为此,提出基于三角形结合方案的 LRCs 构造方法,可构造具有任意 (r, t) 局部性的二元最优 LRCs.性能分析结果表明,构造的可用性 $t=2$ 的 LRCs 达到了最优码率界,构造的具有任意局部性 $r>2$ 和可用性 $t>2$ 的 LRCs 达到了最优最小距离界.与基于近正则图及基于直积码等构造方法相比,本文构造出的 LRCs 在码率上表现更优且参数选择更灵活.

关键词: 分布式存储系统;局部修复码;三角形结合方案;最小距离

中图分类号: TN911.2

文献标志码: A

Construction of Optimal Locally Repairable Codes of Triangular Association Schemes

WANG Jing, LI Jinghui, YANG Jiarong, WANG E

(School of Information Engineering, Chang'an University, Xi'an 710018, China)

Abstract: As a new erasure code for distributed storage systems, locally repairable codes (LRCs) can effectively realize the reliable and efficient storage of massive data. The construction of locally repairable codes with (r, t) locality has become a research hotspot recently. Therefore, the construction methods of locally repairable codes based on triangular association schemes are proposed, which can construct optimal binary locally repairable codes with arbitrary (r, t) locality. Performance analyses show that the LRCs constructed with availability $t=2$ reach the optimal code rate bound, the LRCs constructed with arbitrary locality $r>2$ and availability $t>2$ reach the optimal minimum distance bound. The LRC constructed in this paper performs better in terms of code rate and more flexible parameter selection than those constructed based on near-regular graphs and direct product codes, etc.

Keywords: distributed storage system; locally repairable code (LRC); triangular association schemes; minimum distance

随着信息技术的发展,数据信息出现爆炸式增长,大型分布式存储系统因海量存储能力、高可扩展性以及低成本等显著优点得到了广泛应用^[1].在分

布式存储系统中,数据存储在多个分布式存储节点中^[2].存储系统在运行过程中难免出现不可预期的故障,为了确保数据存储的可靠性,通常采取数据冗

收稿日期: 2023-04-21 修回日期: 2023-09-22 录用日期: 2023-09-25

基金项目: 国家自然科学基金(62001059),陕西省自然科学基金资助项目(2022JM-056),长安大学大学生创新创业训练计划项目(S202310710121)

作者简介: 王 静(1982—),博士,教授,从事网络编码及分布式存储编码等方面的研究; E-mail: jingwang@chd.edu.cn.

余技术. 三副本技术需要很大的存储开销, 纠删码技术能够降低存储开销, 但会耗费大量的网络带宽. Papailiopoulos 等^[3]提出局部修复码 (locally repairable codes, LRCs), 既可以降低故障节点修复过程中所需的存活节点数量, 又可以降低故障节点的修复带宽开销.

如果一个编码符号可以通过访问最多 r 个其他编码符号来恢复, 那么该编码符号具有修复局部性, 该参数用 r 表示, 这 r 个编码符号的集合称为修复集^[4-5]. Gopalan 等^[5]提出了修复局部性 r , 这一参数是衡量修复效率的重要指标, 对于信息符号具有局部性 r 的 LRCs, 给出了码的最小距离上界. 文献^[6-9]中给出了最小距离达到此上界的 LRCs 的相关构造. 除了局部性 r 外, LRCs 的另一个重要特性是可用性. 如果一个编码符号具有 t 个修复集, 那么称该编码符号具有可用性, 该参数用 t 表示. 这个特性与热数据密切相关, 具有可用性的 LRCs 可以确保对热数据进行并行读取和多路径修复^[10]. 为了在多个节点故障的情况下实现局部恢复, Rawat 等^[11]提出了 (r, t) 局部性的概念, 并且证明了信息符号具有 (r, t) 局部性的单校验 LRCs 最小距离的上界. Tamo 等^[12]提出并证明了所有符号具有 (r, t) 局部性的 LRCs 的最小距离和码率上界.

目前大量文献对具有 (r, t) 局部性的 LRCs 构造进行研究. 文献^[12]中基于 t 个二进制 $(r+1, r)$ 奇偶校验码的直积, 构造具有 (r, t) 局部性的二元局部修复码 (binary locally repairable codes, BLRCs), 该 BLRCs 虽然能够实现任意的局部性 r 和可用性 t , 但是其码率较小. 文献^[13]中利用有限域上的迹函数构造了一类循环 (r, t) 局部修复码, 构造出的 BLRCs 达到了最优最小距离, 但是此构造方法只能构造特定参数的 BLRCs 且码率较小. Hao 等^[14]采用有限几何低密度奇偶校验码 (LDPC) 和阵列 LDPC 构造了具有 (r, t) 局部性的 BLRCs, 该 BLRCs 虽然达到了最优最小距离, 不足之处是参数条件限制较多且码率较小. 文献^[15]中基于分区和特定结构的函数构造了两种具有严格可用性 t 的 BLRCs, 然而提出的两种 LRCs 只在某些参数条件下存在. 文献^[16]中基于超图构造的 BLRCs 达到了最优最小距离界, 但是超图的存在需要满足一些参数条件的限制, 参数选择不够灵活, 并且码率较小.

为了解决上述 LRCs 构造中存在的参数限制较多且码率较小的问题, 基于三角形结合方案, 提出具有 (r, t) 局部性的最优 BLRCs 的构造方法. 首先利用三角形结合方案的结合关系, 基于校验矩阵构造

可用性 $t=2$ 的 BLRCs, 进一步基于生成矩阵构造局部性 $r=2$ 的 BLRCs; 为了使 BLRCs 的参数选择更加灵活, 对基于三角形结合方案构造的 BLRCs 进行扩展, 构造能够实现任意局部性 $r>2$ 和任意可用性 $t>2$ 的 BLRCs. 通过性能分析, 基于三角形结合方案构造的具有 $(r, 2)$ 局部性的 BLRCs 达到了最优码率界, 构造的具有任意局部性 $r>2$ 和可用性 $t>2$ 的 BLRCs 达到了最优最小距离界. 与基于近正则图构造的 BLRCs 和基于直积码构造的 BLRCs 等方法相比, 本文 BLRCs 在码率上表现更优且参数选择更灵活.

1 预备知识

1.1 局部修复码

设 C 是有限域 F_q 上的 (n, k) 线性码, 其中 n 为码长, k 为维度. 给定 $[n] = \{1, 2, \dots, n\}$, $c = (c_1, c_2, \dots, c_n)$ 是一个码字, 下面给出具有 (r, t) 局部性的码 C 定义.

定义 1^[11] 如果编码符号 c_i 具有 (r, t) 局部性, 那么需要满足下列条件:

- (1) 存在 t 个子集, 满足 $\varphi_1(i), \dots, \varphi_t(i) \subset [n] \setminus \{i\}$, 需 c_i 能够从 $\varphi_j(i)$ ($j \in [t]$) 中恢复出来, $\varphi_j(i)$ ($j \in [t]$) 称为 c_i 的修复集.
- (2) $|\varphi_j(i)| \leq r, j \in [t]$.
- (3) $\varphi_j(i) \cap \varphi_l(i) = \emptyset, j \neq l \in [t]$.

如仅有信息符号具有 (r, t) 局部性, 则此码称作 $(n, k, r, t)_i$ LRCs. 如所有符号具有 (r, t) 局部性, 则此码称作 $(n, k, r, t)_a$ LRCs.

定义 2^[15] 对于 $\mathbf{v} = [v_1 \ v_2 \ \dots \ v_n] \in F_q^n$, \mathbf{v} 中非零元素下标的集合为 \mathbf{v} 的支持集, 记作 $\text{supp}(\mathbf{v})$, 即

$$\text{supp}(\mathbf{v}) = \{i \in [n]: v_i \neq 0\} \tag{1}$$

定理 1^[17] 对于信息位具有 (r, t) 局部性的 (n, k, d) LRCs, 最小距离应满足:

$$d \geq t + 1 \tag{2}$$

定理 2^[11] 若 LRCs 的所有信息位码元的每个修复集中只包含一个校验位, 那么该单校验 $(n, k, r, t)_i$ LRCs 的最小距离满足:

$$d \leq n - k - \left\lceil \frac{kt}{r} \right\rceil + t + 1 \tag{3}$$

称达到边界式 (3) 的 LRCs 是最小距离最优的单校验 $(n, k, r, t)_i$ LRCs.

定理 3^[13] 若 (n, k, r, t) LRCs 的每个码元具有 t 个大小为 r 的不相交修复集, 那么该码码率满足:

$$R \leq \frac{1}{\prod_{i=1}^t \left(1 + \frac{1}{ir}\right)} \quad (4)$$

称达到边界式(4)的 LRCs 是码率最优的 (n, k, r, t) LRCs.

定理 4 特别地, Prakash 等^[18]进一步提出了 $(n, k, r, t=2)$ LRCs 的码率上界:

$$R \leq \frac{r}{r+2} \quad (5)$$

称达到边界式(5)的 LRCs 是码率最优的 $(n, k, r, 2)$ LRCs.

定理 5 对于具有严格可用性的 LRCs, Balaji 等^[19]提出其码长需要满足:

$$n \geq (r+1)^2 - \frac{r(r+1)}{t} \quad (6)$$

1.2 三角形结合方案

结合方案是关于集合 Ω 中元素对之间的关系, $\Omega \times \Omega$ 是 Ω 中有序元素对的集合, 即 $\Omega \times \Omega = \{(\alpha, \beta) : \alpha \in \Omega, \beta \in \Omega\}$. 令 B 是 $\Omega \times \Omega$ 的任意子集, 其对偶子集是 B' , 其中 $B' = \{(\beta, \alpha) : (\alpha, \beta) \in B\}$, 如果 $B = B'$, 则称 B 是对称的. 一个特殊的对称子集是对角子集, 对角子集 $\text{Diag}(\Omega)$ 可以表示为 $\text{Diag}(\Omega) = \{(\omega, \omega) : \omega \in \Omega\}$.

定义 3^[20] 称为结合方案. 有限集 Ω 上具有 s 个结合类的结合方案是将 $\Omega \times \Omega$ 划分成集合 D_0, D_1, \dots, D_s , 称为结合类, 满足以下条件:

- (1) $D_0 = \text{Diag}(\Omega)$.
- (2) D_i 是对称的, 其中 $i=1, 2, \dots, s$.
- (3) 对于 $\{0, 1, \dots, s\}$ 中所有的 i, j, k , 有正整数 p_{ij}^k , 对 D_k 中所有 (α, β) , 满足

$$|\{\gamma \in \Omega : (\alpha, \gamma) \in D_i, (\gamma, \beta) \in D_j\}| = p_{ij}^k$$

定义 4^[20] 称为三角形结合方案. 设 Ω 是由 m 元集 Γ 中所有二元子集构成的集合族, 对于 Ω 中的元素 α , 令

$$D_1(\alpha) = \{\beta \in \Omega : |\alpha \cap \beta| = 1\}$$

$$D_2(\alpha) = \{\beta \in \Omega : \alpha \cap \beta = \emptyset\}$$

若 $\beta \in D_1(\alpha)$, 即满足 $|\alpha \cap \beta| = 1$, 则称 α 与 β 具有第一类结合关系; 若 $\beta \in D_2(\alpha)$, 则称 α 与 β 具有第二类结合关系, 即三角形结合方案.

2 基于三角形结合方案构造 BLRCs

基于三角形结合方案中的结合关系可构造可用性 $t=2$ 的 BLRCs, 进一步基于生成矩阵可构造出局部性 $r=2$ 的 BLRCs; 为了使 BLRCs 的参数更加灵活, 对基于三角形结合方案构造的 BLRCs 进行扩展, 进一步构造能够实现任意局部性 $r>2$ 和任意可

用性 $t>2$ 的 BLRCs.

2.1 构造可用性 $t=2$ 的 BLRCs

首先基于三角形结合方案构造关联矩阵, 基于关联矩阵构造可用性 $t=2$ 的 BLRCs. 通过构造生成矩阵进一步得到局部性 $r=2$ 的 BLRCs. 构造关联矩阵的具体步骤如下:

步骤 1 用 Ω 表示三角形结合方案中 $m+1$ 元集 $\Gamma = \{1, 2, \dots, m+1\}$ 全部二元子集构成的集合族, 则此集合族中共有 $m(m+1)/2$ 个元素, 其中 $m \geq 2$.

步骤 2 对任意二元子集 $L \in \Omega$, 令 $B_i = \{L \mid i \in L\}$, $B = \{B_1, B_2, \dots, B_{m+1}\}$, 其中 $i \in \Gamma$.

步骤 3 构造关联矩阵

$\mathbf{M} = [m_{ij}]$, $1 \leq i \leq m+1, 1 \leq j \leq m(m+1)/2$ 其中

$$m_{ij} = \begin{cases} 1, & \Omega_j \in B_i \\ 0, & \Omega_j \notin B_i \end{cases}$$

由 $|B_i| = m$ 可知, 关联矩阵 \mathbf{M} 的行重为 m ; 对任意二元子集 $L \in \Omega$, 必定存在 B_{i_1} 及 B_{i_2} , 其中 $i_1 \neq i_2$, $i_1, i_2 \in \Gamma$, 使得 $L \in B_{i_1}$ 且 $L \in B_{i_2}$, 可知关联矩阵 \mathbf{M} 的列重为 2. 因此, 关联矩阵 \mathbf{M} 可以表示为 $(m+1) \times (m(m+1)/2)$ 阶的二元稀疏 ($r=m, t=2$) - 正则矩阵.

基于以上关联矩阵构造校验矩阵, 考虑由校验矩阵定义二条码, 有如下构造.

构造 1 由校验矩阵 $\mathbf{H}_1 = [\mathbf{M} \mid \mathbf{I}_{(m+1)}]$ 构造的码 C_1 是所有符号具有局部性 r 和可用性 t 的单校验 $(n, k, r, t)_a$ BLRCs, 其中满足参数条件

$$n = \frac{(m+1)(m+2)}{2}$$

$$k = \frac{m(m+1)}{2}$$

$$r = m, t = 2$$

证明 由文献[15]可知, 如果 C 中的每个码元符号 $c_i (i \in [n])$, 在对偶码中都存在 t 个码字 $\mathbf{h}_1^i, \mathbf{h}_2^i, \dots, \mathbf{h}_t^i$, 每个码字汉明重量 $\leq r+1$, 且 $\text{supp}(\mathbf{h}_g^i) \cap \text{supp}(\mathbf{h}_l^i) = \{i\}$, $\forall 1 \leq g \neq l \leq t$, 那么码 C 被称为所有符号具有可用性 t 的 LRCs. 从校验矩阵 \mathbf{H}_1 可以确定码 C_1 的码长、维度和所有符号局部性. 接下来证明码 C 的所有符号具有可用性 $t=2$.

对于码元符号 $c_i (i \in [1, k])$, 校验矩阵 \mathbf{H}_1 在第 i 列非零的 2 行即为满足上述条件的 2 个码字. 将校验矩阵 \mathbf{H}_1 的所有行相加, 可以得到对偶码 C^\perp 的一个码字 $c^\perp = (\mathbf{0}_{\frac{m(m+1)}{2}}, \mathbf{1}_{m+1})$. 对于码元符号 $c_i (i \in [k+1, n])$, 校验矩阵在第 i 列非零的行与

码字 c^\perp 即为满足上述条件的两个码字. 因此, 码 C_1 具有所有符号可用性 $t = 2$.

例 1 以 $m = 4$ 为例构造可用性 $t = 2$ 的 BLRCs, 则 $\Gamma = \{1, 2, 3, 4, 5\}, \Omega = \{(i, j) \mid i < j \in \Gamma\}, B = \{\{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}\}, \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{2, 5\}\}, \{\{1, 3\}, \{2, 3\}, \{3, 4\}, \{3, 5\}\}, \{\{1, 4\}, \{2, 4\}, \{3, 4\}, \{4, 5\}\}, \{\{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}\}$, 将 B 中元素与矩阵的行关联, 将 Ω 中元素与矩阵的列关联, 那么可知关联矩阵 \mathbf{M} 是一个 5×10 阶的正则矩阵, 关联矩阵 \mathbf{M} 可具体表示如下:

$$\mathbf{M} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

由校验矩阵 $\mathbf{H}_1 = [\mathbf{M} \mid \mathbf{I}_5]$ 构造的码是所有符号具有局部性 r 和可用性 t 的 $(n = 15, k = 10, r = 4, t = 2)$ BLRCs, 码的最小距离 $d = 3$. 若信息位 c_1 发生故障, 则由 BLRCs 的校验矩阵 \mathbf{H}_1 可知, 信息位 c_1 可用 $c_1 = c_{11} - c_2 - c_3 - c_4 = c_{12} - c_5 - c_6 - c_7$ 来恢复, 那么信息位 c_1 的修复集可表示为

$$\varphi_1(1) = \{2, 3, 4, 11\}, \varphi_2(1) = \{5, 6, 7, 12\}$$

每个信息符号的修复集均含有一个校验位符号. 若校验位 c_{11} 发生故障, 则由 BLRCs 的校验矩阵 \mathbf{H}_1 可知, 校验位 c_{11} 可用 $c_{11} = c_1 + c_2 + c_3 + c_4 = c_{12} + c_{13} + c_{14} + c_{15}$ 来恢复, 那么校验位 c_{11} 的修复集可表示为

$$\varphi_1(11) = \{1, 2, 3, 4\}, \varphi_2(11) = \{12, 13, 14, 15\}$$

可以看出校验符号同样具有两种修复方式.

推论 1 由生成矩阵

$$\mathbf{G} = [\mathbf{I}_{m+1} \mid \mathbf{M}]$$

定义的码 C_2 是所有符号具有局部性 r 和可用性 t 的单校验 (n, k, r, t) BLRCs, 其中参数满足条件

$$\begin{aligned} n &= (m+1)(m+2)/2 \\ k &= m+1, r=2, t=m \end{aligned}$$

证明 该推论的证明与构造 1 相似.

推论 2 由关联矩阵 \mathbf{M} 作为校验矩阵定义的码 C_3 是所有符号具有严格可用性的 (n, k, r, t) BLRCs, 其中参数满足条件

$$\begin{aligned} n &= m(m+1)/2, k=(m-1)m/2 \\ r &= m-1, t=2 \end{aligned}$$

且构造的 BLRCs 的码长达到了 Balaji 等^[19] 提出的具有严格可用性的 BLRCs 的码长界.

证明 若 $a \times b$ 阶校验矩阵的行重为 $r+1$, 列重

为 t , 满足 $bt = a(r+1)$, 且校验矩阵中第 i 列具有非零项的行的支持集由 $S_j^{(i)}, j = 1, 2, \dots, t$ 给出, 满足

$$S_j^{(i)} \cap S_l^{(i)} = \{i\}, \forall 1 \leq j \neq l \leq t$$

由此类校验矩阵构造的码称为具有严格可用性 t 的码^[15]. 因此, 由关联矩阵 \mathbf{M} 作为校验矩阵定义的码是具有严格可用性的码.

由关联矩阵 \mathbf{M} 的形式可以确定码 C_3 的码长、所有符号局部性和可用性. 然后对码 C_3 的维度进行证明. 由于构造的关联矩阵 \mathbf{M} 的秩为行数减 1, 所以码 C_3 的维度

$$\begin{aligned} k &= n - \text{rank}(\mathbf{M}) = m(m+1)/2 - (m+1-1) = \\ &= (m-1)m/2 \end{aligned}$$

由码 C_3 的参数条件可知

$$\begin{aligned} (r+1)^2 - r(r+1)/t &= m^2 - (m-1)m/2 = \\ &= m(m+1)/2 = n \end{aligned}$$

即构造出的码长达到了 Balaji 等^[19] 提出的具有严格可用性的码具有的码长界.

2.2 构造具有任意局部性和可用性的 BLRCs

现有码结构主要是针对给定参数的系统, 因此缺乏适应系统参数变化的能力. 使用构造 1 仅能构造可用性 $t=2$ 的 BLRCs. 本文对构造 1 进行推广, 进一步构造具有任意局部性 $r>2$ 和可用性 $t>2$ 的 BLRCs.

矩阵构造示意图如图 1 所示. 用 $\Phi_{m,p}$ 表示行重为 m 、列重为 p 的正则矩阵. 由于基于三角形结合方案构造的关联矩阵 \mathbf{M} 的行重为 m , 列重为 2, 因此, 用 $\Phi_{m,2}$ 表示行重为 m 的关联矩阵 \mathbf{M} . 当 $m, p > 2$ 时, 给定 m, p , 使用矩阵

$$\Phi_{m,p} = \begin{bmatrix} \Phi_{m,p-1} & \mathbf{0} \\ \mathbf{I} & \Phi_{p,m-1}^T \end{bmatrix}$$

可进一步构造行重为 m 、列重为 p 的正则矩阵. 矩阵 $\Phi_{m,p}$ 中的块最终均能用 $\Phi_{l,2} (2 \leq l \leq m), \Phi_{v,2}^T (2 \leq v \leq p)$ 、单位矩阵及零矩阵表示. 例如, 由 $\Phi_{3,2}, \Phi_{3,2}^T$ 、单位矩阵及零矩阵可表示出 $\Phi_{3,3}$, 即

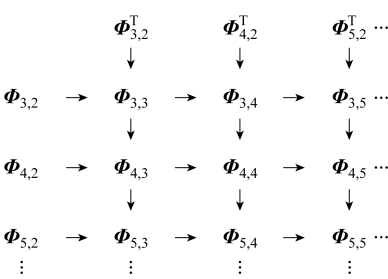


图 1 矩阵构造示意图

Fig. 1 Diagram of matrix construction

$$\Phi_{3,3} = \begin{bmatrix} \Phi_{3,2} & \mathbf{0} \\ \mathbf{I} & \Phi_{3,2}^T \end{bmatrix}$$

其中： $\Phi_{3,2}$ 即为由三角形结合方案构造得到的行重为 3、列重为 2 的关联矩阵。

构造 2 由校验矩阵

$$H_2 = \left[\begin{array}{cc|c} \Phi_{m,p-1} & \mathbf{0} & \\ \hline \mathbf{I} & \Phi_{p,m-1}^T & \mathbf{I} \end{array} \right]$$

定义的码 C_4 是信息符号,可以实现任意局部性 $r > 2$ 和任意可用性 $t > 2$ 的 $(n = (m + 1)(m + 2) \cdots (m + p)/p!, k = m(m + 1) \cdots (m + p - 1)/p!, r = m, t = p)$ BLRCs.

证明 首先计算矩阵 $\Phi_{m,p}$ 的大小.由构造 1 可知 $\Phi_{m,2}$ 的行数为 $m + 1$,列数为 $m(m + 1)/2$.由于矩阵 $\Phi_{3,m-1}^T$ 与 $\Phi_{m-1,3}$ 的行数及列数相同,当 $p = 3$ 时,为了计算方便,使用如下矩阵计算 $\Phi_{m,3}$ 的行数和列数:

$$\begin{bmatrix} \Phi_{m,2} & \mathbf{0} \\ \mathbf{I} & \Phi_{m-1,3} \end{bmatrix} = \begin{bmatrix} \Phi_{m,2} & \mathbf{0} \\ \hline \mathbf{I} & \begin{bmatrix} \Phi_{m-1,2} & \mathbf{0} \\ \hline \ddots & \ddots \\ \hline \mathbf{I} & \begin{bmatrix} \Phi_{4,2} & \mathbf{0} \\ \hline \mathbf{I} & \begin{bmatrix} \Phi_{3,2} & \mathbf{0} \\ \hline \mathbf{I} & \Phi_{2,3} \end{bmatrix} \end{bmatrix} \end{bmatrix}$$

根据矩阵形式, $\Phi_{m,3}$ 的行数可表示为

$$m + 1 + \frac{m(m + 1)}{2} = \frac{(m + 1)(m + 2)}{2}$$

$\Phi_{m,3}$ 的列数可表示为

$$\frac{(m + 1)m}{2} + \frac{m(m - 1)}{2} + \cdots + \frac{4 \times 3}{2} + 4 = \frac{m(m + 1)(m + 2)}{2 \times 3}$$

$\Phi_{m,4}$ 的行数可表示为

$$\frac{(m + 1)(m + 2)}{2} + \frac{m(m + 1)(m + 2)}{6} = \frac{(m + 1)(m + 2)(m + 3)}{2 \times 3}$$

$\Phi_{m,4}$ 的列数可表示为

$$\frac{(m + 2)(m + 1)m}{6} + \frac{(m + 1)m(m - 1)}{6} + \cdots + \frac{5 \times 4 \times 3}{6} + 5 = \frac{m(m + 1)(m + 2)(m + 3)}{2 \times 3 \times 4}$$

当 $p > 2$ 时,假设 $\Phi_{m,p}$ 的行数为 $(m + 1)(m + 2) \cdots (m + p - 1)/(p - 1)!$, $\Phi_{m,p}$ 的列数为 $m(m + 1) \cdots (m + p - 1)/p!$.由于矩阵 $\Phi_{p+1,m-1}^T$ 与 $\Phi_{m-1,p+1}$ 的行数及列数相同,为了计算方便,使用如下矩阵计

算 $\Phi_{m,p+1}$ 的行数和列数:

$$\begin{bmatrix} \Phi_{m,p} & \mathbf{0} \\ \mathbf{I} & \Phi_{m-1,p+1} \end{bmatrix} = \begin{bmatrix} \Phi_{m,p} & \mathbf{0} \\ \hline \mathbf{I} & \begin{bmatrix} \Phi_{m-1,p} & \mathbf{0} \\ \hline \ddots & \ddots \\ \hline \mathbf{I} & \begin{bmatrix} \Phi_{4,p} & \mathbf{0} \\ \hline \mathbf{I} & \begin{bmatrix} \Phi_{3,p} & \mathbf{0} \\ \hline \mathbf{I} & \Phi_{2,p+1} \end{bmatrix} \end{bmatrix} \end{bmatrix}$$

矩阵 $\Phi_{m,p+1}$ 的行数为

$$\frac{(m + 1)(m + 2) \cdots (m + p - 1)}{(p - 1)!} + \frac{m(m + 1) \cdots (m + p - 1)}{p!} = \frac{(m + 1)(m + 2) \cdots (m + p)}{p!}$$

矩阵 $\Phi_{m,p+1}$ 的列数为

$$\frac{m(m + 1) \cdots (m + p - 1)}{p!} + \frac{(m - 1)m \cdots (m + p - 2)}{p!} + \cdots + \frac{3 \times 4 \cdots (p + 2)}{p!} + p + 2 = \frac{m(m + 1) \cdots (m + p)}{(p + 1)!}$$

假设成立.

因此,当 $p > 2$ 时, $\Phi_{m,p}$ 的行数为 $(m + 1)(m + 2) \cdots (m + p - 1)/(p - 1)!$, $\Phi_{m,p}$ 的列数为 $m(m + 1) \cdots (m + p - 1)/p!$.则由校验矩阵 $H_2 = [\Phi_{m,p} \mid \mathbf{I}]$ 定义的码长

$n = (m + 1)(m + 2) \cdots (m + p)/p!$

维度

$$k = m(m + 1) \cdots (m + p - 1)/p!$$

当需要构造给定局部性 r 及可用性 t 的 BLRCs 时,可以基于三角形结合方案构造所需的列重为 2 的关联矩阵,由这些关联矩阵构造得到校验矩阵 $H_2 = [\Phi_{r,t} \mid \mathbf{I}]$ 进而构造 BLRCs.

例 2 以 $r = 3, t = 5$ 为例构造 BLRCs,由上述构造方法可知:

$$\Phi_{3,5} = \begin{bmatrix} \Phi_{3,4} & \mathbf{0} \\ \mathbf{I} & \Phi_{5,2}^T \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} \Phi_{3,3} & \mathbf{0} \\ \hline \mathbf{I} & \Phi_{4,2}^T \end{bmatrix} & \mathbf{0} \\ \hline \mathbf{I} & \Phi_{5,2}^T \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} \Phi_{3,2} & \mathbf{0} \\ \hline \mathbf{I} & \Phi_{3,2}^T \end{bmatrix} & \mathbf{0} \\ \hline \mathbf{I} & \begin{bmatrix} \Phi_{4,2}^T \\ \hline \mathbf{I} & \Phi_{5,2}^T \end{bmatrix} \end{bmatrix}$$

其中,基于三角形结合方案构造关联矩阵的方法,矩阵 $\Phi_{3,2}$ 可以表示为

$$\Phi_{3,2} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

矩阵 $\Phi_{4,2}$ 、 $\Phi_{5,2}$ 也同样可以表示出来,可以看出,矩阵 $\Phi_{3,5}$ 中的块最终能用 $\Phi_{3,2}$ 、 $\Phi_{3,2}^T$ 、 $\Phi_{4,2}^T$ 、 $\Phi_{5,2}^T$ 、单位矩阵及零矩阵表示.由校验矩阵 $H_2 = [\Phi_{3,5} | I]$ 定义的码是信息符号可以实现局部性和可用性的 $(n=56, k=21, r=3, t=5)_i$ BLRCs.

3 性能分析

3.1 最小距离

定理 6 由构造 1 中校验矩阵 H_1 构造得到的 $(n, k, r, 2)_a$ BLRCs 的最小距离为 $d = 3$.

证明 通过观察构造 1 中校验矩阵 H_1 可知,由于关联矩阵 M 的列重为 2,且关联矩阵 M 的右边是一个单位矩阵,所以校验矩阵 H_1 中存在线性相关的 3 列.因此,构造得到的 LRCs 的最小距离 $d \leq 3$.另一方面,从校验矩阵中任取两列,若两列都来自关联矩阵 M 或两列都来自单位矩阵 $I_{(m+1)}$,显然它们线性无关;若一列来自关联矩阵 M ,另一列来自单位矩阵 $I_{(m+1)}$,由于列重不同,它们必然线性无关.因此,构造得到的 BLRCs 的最小距离 $d \geq 3$.综上所述可知,构造 1 构造的 BLRCs 的最小距离为 $d = 3$.

定理 7 由构造 2 中校验矩阵 H_2 构造得到的信息符号可以实现任意局部性 $r > 2$ 和任意可用性 $t > 2$ 的 $(n, k, r, t)_i$ BLRCs 是最小距离最优的 BLRCs,且码的最小距离 $d = t + 1$.

证明 由构造 2 中的校验矩阵 H_2 可知,矩阵 $\Phi_{m,p}$ 的列重为 p ,且矩阵 $\Phi_{m,p}$ 的右边是一个单位矩阵,可知从矩阵 $\Phi_{m,p}$ 中任选一列是单位阵中 p 列的

线性组合,即校验矩阵 H_2 中存在线性相关的 $p + 1$ 列.因此,由校验矩阵 H_2 构造得到的 BLRCs 的最小距离 $d \leq p + 1$.另一方面,根据矩阵 $\Phi_{m,p}$ 的形式可知,矩阵 $\Phi_{m,p}$ 的行重为 m ,列重为 p ,每列“1”元素所在 p 行中任意两行的支撑集只在该元素处相交,因此每个信息符号的修复局部性为 m 且具有 p 个不相交的修复集.根据定理 1,最小距离应满足 $d \geq p + 1$.综上所述,可知由校验矩阵 H_2 构造所得的 BLRCs 的最小距离 $d = p + 1$.

又因为由校验矩阵 H_2 构造的 BLRCs 的参数满足

$$\begin{aligned} n &= (m+1)(m+2)\cdots(m+p)/p! \\ k &= m(m+1)\cdots(m+p-1)/p! \\ r &= m, \quad t = p \end{aligned}$$

将这些参数代入式(3),可得:

$$\begin{aligned} d &\leq n - k - \left\lceil \frac{kt}{r} \right\rceil + t + 1 = \\ &= \frac{(m+1)(m+2)\cdots(m+p)}{p!} - \\ &\quad \frac{m(m+1)\cdots(m+p-1)}{p!} - \\ &\quad \left\lceil \frac{m(m+1)\cdots(m+p-1)}{p!} \frac{p}{m} \right\rceil + p + 1 = p + 1 \end{aligned}$$

因为 $p = t$,所以构造出的 BLRCs 的最小距离 $d = t + 1$,且达到了式(3)中的最小距离边界,即该码是最小距离最优的 BLRCs,证毕.

3.2 构造参数分析

由表 1 可知,当可用性 $t = 2$ 时,有

$$\frac{r}{r+2} > \left(\frac{r}{r+1} \right)^2$$

即由构造 1 构造的 BLRCs 的码率高于基于直积码构造的 BLRCs 的码率.虽然基于直积码构造的 BLRCs 的最小距离大于构造 1 构造的 BLRCs 最小距离,但当局部性 $r > 1$ 时,由于

表 1 构造 1 参数比较分析

Tab. 1 Comparative analysis of parameters of Construction 1

构造方式	构造参数	最小距离	相对距离
构造 1 构造的 BLRCs	$n = \frac{(r+1)(r+2)}{2}, k = \frac{r(r+1)}{2}, r, t = 2$	$d_{\min} = 3$	$\frac{6}{(r+1)(r+2)}$
基于近正则图构造的 BLRCs ^[18]	$n = k + \left\lceil \frac{2k}{r} \right\rceil, \left\lceil \frac{2k}{r} \right\rceil \geq r + 2, t = 2$	$d_{\min} = 3$	$\frac{3}{k + \left\lceil \frac{2k}{r} \right\rceil}$
基于单位矩阵变换构造的 BLRCs ^[21]	$n = r^2 + 2r, k = r^2, r, t = 2$	$d_{\min} = 3$	$\frac{3}{r(r+2)}$
基于直积码构造的 BLRCs ^[12] ($t=2$)	$n = (r+1)^2, k = r^2, r, t = 2$	$d_{\min} = 4$	$\frac{4}{(r+1)^2}$

$$\frac{6}{(r+1)(r+2)} > \frac{4}{(r+1)^2}$$

即构造 1 构造的 BLRCs 的相对距离大于基于直积码构造的 BLRCs 的相对距离. 当 $r \mid 2k$ 且 $2k = r(r+2)$ 时, 基于近正则图构造的 BLRCs 的相对距离

$$\frac{6}{(r+2)^2} < \frac{6}{(r+1)(r+2)}$$

即基于近正则图构造的 BLRCs 的相对距离小于构造 1 构造的 BLRCs. 构造 1 构造的 BLRCs 与基于单位矩阵变换构造的 BLRCs 能够达到相同的最小距离和码率, 但是当局部性 r 取相同值并且 $r > 1$ 时, 可知其相对距离

$$\frac{6}{(r+1)(r+2)} > \frac{3}{r(r+2)}$$

即构造 1 构造的 BLRCs 的相对距离大于基于单位矩阵变换构造的 BLRCs.

图 2 给出了构造 1 构造的 BLRCs、基于近正则图、基于直积码构造的 BLRCs 的码率 R 随局部性 r 变化曲线以及 Prakash 等^[18] 提出的码率上界曲线. 可以看出, 当可用性 $t=2$ 时, 随着局部性 r 的增大, 码率同时呈增大的趋势; 当局部性 r 取相同值时, 构

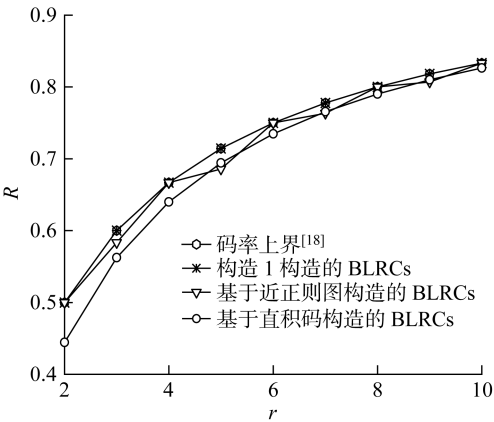


图 2 可用性 $t=2$ 时码率随局部性的变化
Fig. 2 Code rate versus locality at availability $t=2$

造 1 构造的 BLRCs 的码率高于基于直积码构造的 BLRCs; 当局部性 r 取奇数时, 构造 1 构造的 BLRCs 的码率高于基于近正则图构造的 BLRCs. 此外, 构造 1 构造的 BLRCs 的码率 $R=r/(r+2)$, 达到了 Prakash 等^[18] 提出的码率上界.

由于推论 1 仅能构造局部性 $r=2$ 的 BLRCs, 将其与基于单纯形码构造的 BLRCs 以及基于直积码构造的 BLRCs 进行比较. 由表 2 可知, 当基于直积码构造的 BLRCs 的局部性取为 $(2, t)$ 且 $t > 1$ 时, 有

$$\frac{2}{2+t} > \left(\frac{2}{3}\right)^t$$

即由推论 1 得到的 BLRCs 的码率高于基于直积码构造的 BLRCs. 此外, 由推论 1 得到的 BLRCs 的相对距离也大于基于直积码构造的 BLRCs. 基于单纯形码仅能构造可用性 $t=2^{m-1}-1$ 的 BLRCs, 限制了可用性的参数选择, 而基于推论 1 可以构造具有任意可用性的 BLRCs.

图 3 给出了局部性 $r=2$ 时, 3 种码的码率 R 随可用性 t 变化曲线以及 Tamo 等^[12] 提出的码率上界曲线. 可以看出, 当局部性 r 一定, 随着可用性 t 的增大, 码率同时呈减小的趋势; 当可用性 t 取相同值

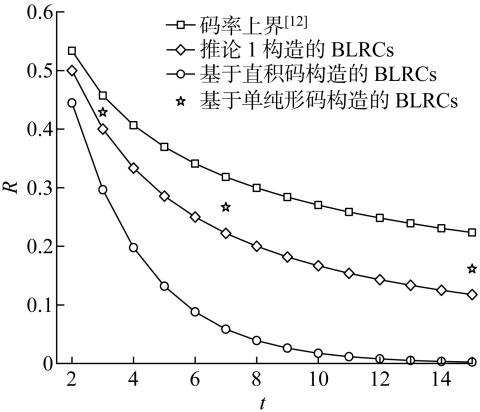


图 3 局部性 $r=2$ 时, 码率随可用性的变化
Fig. 3 Code rate versus availability at locality $r=2$

表 2 推论 1 参数比较分析

Tab. 2 Comparative analysis of parameters of Corollary 1

构造方式	构造参数	最小距离	相对距离
推论 1 构造的 BLRCs	$n = \frac{(t+1)(t+2)}{2}, k = t+1, r = 2, t$	$d_{\min} = t+1$	$\frac{2}{t+2}$
基于单纯形码构造的 BLRCs ^[22]	$n = 2^m - 1, k = m, r = 2, t = 2^{m-1} - 1$	$d_{\min} = t+1$	$\frac{t+1}{2t+1}$
基于直积码构造的 BLRCs ^[12] ($r = 2$)	$n = 3^t, k = 2^t, r = 2, t$	$d_{\min} = 2^t$	$\left(\frac{2}{3}\right)^t$

时,推论 1 构造的 BLRCs 的码率高于基于直积码构造的 BLRCs. 虽然基于单纯形码构造的 BLRCs 的码率高于推论 1 构造的 BLRCs,但是其可用性 t 具有较大的参数限制,推论 1 构造的 BLRCs 的参数选择更加灵活.

由构造 2 可以构造任意局部性 $r>2$ 和可用性 $t>2$ 的 BLRCs,将其与基于迹函数构造的 BLRCs、

基于超图构造的 BLRCs、基于阵列 LDPC 码构造的 BLRCs 以及基于直积码构造的 BLRCs 进行比较. 由表 3 可知,将码的局部性都取为 (r,t) ,当 $t > 2$ 时,可知

$$\left(1+\frac{1}{r}\right)^t>1+\frac{t}{r}$$

因此基于直积码构造的 BLRCs 的码率

表 3 构造 2 构造参数比较分析
Tab. 3 Comparative analysis of parameters of Construction 2

构造方式	n	k	r	t	R
构造 2 构造的 BLRCs	$\frac{(r+1)(r+2)\cdots(r+t)}{t!}$	$\frac{r(r+1)\cdots(r+t-1)}{t!}$	$r>2$	$t>2$	$\frac{r}{r+t}$
基于迹函数构造的 BLRCs ^[13]	2^m-1	$2^{m-1}-1$	$m-1$	m	$\frac{2^r-1}{2^{r+1}-1}$
基于超图构造的 BLRCs ^[16]	$v+\frac{1}{r}vt$	v	$v\geq t(r-1)+1, r vt$		$\frac{r}{r+t}$
基于阵列 LDPC 码构造的 BLRCs ^[14]	r^2+rt+1	r^2	r (奇素数)	t (偶数)	$\frac{r^2}{r^2+rt+1}$
基于直积码构造的 BLRCs ^[12]	$(r+1)^t$	r^t	r	t	$\left(\frac{r}{r+1}\right)^t$

$$\left(\frac{r}{r+1}\right)^t=\frac{1}{\left(\frac{r+1}{r}\right)^t}<\frac{1}{1+\frac{t}{r}}=\frac{r}{r+t}$$

经分析可知,构造 2 构造的 BLRCs 的码率总高于基于直积码构造的 BLRCs. 由于

$$\frac{r}{r+t}>\frac{r^2}{r^2+rt+1}$$

即构造 2 构造的 BLRCs 的码率总高于基于阵列 LDPC 码构造的 BLRCs. 基于迹函数构造出的 BLRCs 需要满足可用性 $t=r+1$,只能构造特定参数的 BLRCs,具有较大的参数限制,并且仅能构造码率 $\frac{2^r-1}{2^{r+1}-1}<\frac{1}{2}$ 的 BLRCs. 基于超图构造的 BLRCs 与构造 2 构造的 BLRCs 码率相同,但是超图存在的必要条件是超图的顶点数 $v\geq t(r-1)+1$ 并且 $r|vt$,基于超图构造出的 BLRCs 具有极大的参数限制,主要针对特定参数的系统.

图 4 所示为当局部性 $r=11$ 时,构造 2 构造的 BLRCs 和几种典型 BLRCs 的码率随可用性的变化曲线,以及 Tamo 等^[12]提出的码率上界曲线. 当局部性 r 一定,随着可用性 t 的增加,码率降低. 当可用性 t 取相同值时,构造 2 构造的 BLRCs 的码率尽管没有达到 Tamo 等^[12]提出的码率上界,但高于基于直积码构造的 BLRCs 的码率. 此外,当局部性

$r=11$ 时,基于阵列 LDPC 码仅能构造可用性 t 取偶数的 BLRCs,具有一定的参数限制. 基于迹函数构造的 BLRCs 的码率略高于构造 2 构造的 BLRCs,但是当局部性 $r=11$ 时,基于迹函数仅能构造可用性 $t=12$ 的 BLRCs,参数选择不够灵活.

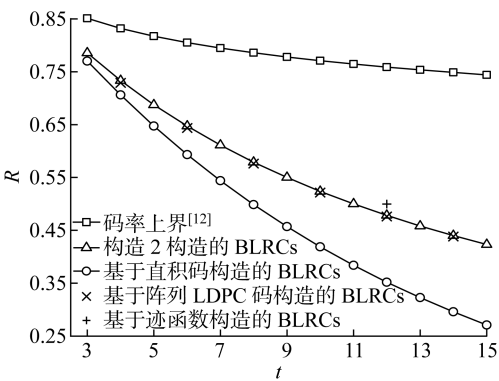


图 4 局部性 $r=11$ 时码率随可用性的变化

Fig. 4 Code rate versus availability at locality $r=11$

当可用性 $t=4$ 时,码率随局部性的变化曲线以及 Tamo 等^[12]提出的码率上界曲线如图 5 所示. 随着局部性 r 的增大,码率同时呈增大的趋势;当局部性 r 取相同值时,构造 2 构造的 BLRCs 的码率仍高于基于直积码构造的 BLRCs. 此外,基于迹函数构造的 BLRCs 的码率高于构造 2 构造的 BLRCs,但

是当可用性 $t=4$ 时,基于迹函数仅能构造局部性 $r=3$ 的 BLRCs,基于阵列 LDPC 码仅能构造局部性 r 取奇素数的 BLRCs,具有一定的参数限制且码率略低于构造 2 构造的 BLRCs.

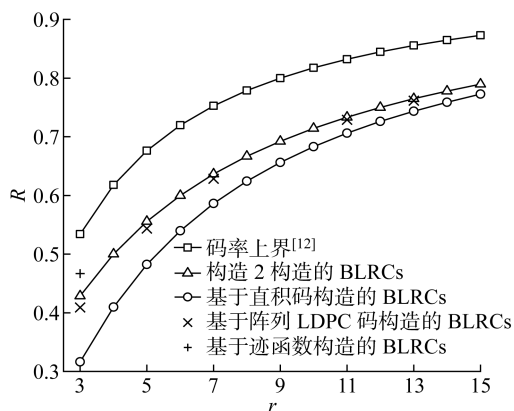


图 5 可用性 $t=4$ 时码率随局部性的变化

Fig. 5 Code rate versus locality at availability $t=4$

4 结语

局部修复码能够有效实现分布式存储系统对海量数据的高可靠、高效率存储。提出基于三角形结合方案及其扩展的 BLRCs 构造方法,可以得到具有任意 (r, t) 局部性 BLRCs。运用三角形结合方案的结合关系,基于校验矩阵构造可用性 $t=2$ 的 BLRCs,进一步基于生成矩阵构造局部性 $r=2$ 的 BLRCs;为了使 BLRCs 的参数选择更加灵活,对基于三角形结合方案构造的 BLRCs 进行扩展,进一步构造能够实现任意局部性 $r>2$ 和任意可用性 $t>2$ 的 BLRCs。构造的具有 $(r, 2)$ 局部性的 BLRCs 达到了最优码率界;构造的具有任意局部性 $r>2$ 和可用性 $t>2$ 的 BLRCs 达到了最优最小距离界。分析表明,与基于近正则图构造的 BLRCs 以及基于直积码构造的 BLRCs 等相比,本文构造的 BLRCs 在码率上表现更优且参数选择更灵活。

参考文献:

[1] FANG W J, CHEN B, XIA S T, *et al.* Singleton-optimal LRCs and perfect LRCs via cyclic codes[C]// **2021 IEEE International Symposium on Information Theory**. Melbourne, Australia: IEEE, 2021: 3261-3266.

[2] YAVARI E, ESMAEILI M. Locally repairable codes: Joint sequential-parallel repair for multiple node failures[J]. **IEEE Transactions on Information Theory**, 2020, 66(1): 222-232.

[3] PAPAILIOPOULOS D S, DIMAKIS A G. Locally repairable codes[J]. **IEEE Transactions on Information Theory**, 2014, 60(10): 5843-5855.

[4] WANG A Y, ZHANG Z F, LIN D D. Bounds for binary linear locally repairable codes via a sphere-packing approach[J]. **IEEE Transactions on Information Theory**, 2019, 65(7): 4167-4179.

[5] GOPALAN P, HUANG C, SIMITCI H, *et al.* On the locality of codeword symbols[J]. **IEEE Transactions on Information Theory**, 2012, 58(11): 6925-6934.

[6] LUO Y, XING C P, YUAN C. Optimal locally repairable codes of distance 3 and 4 via cyclic codes[J]. **IEEE Transactions on Information Theory**, 2019, 65(2): 1048-1053.

[7] JIN L F. Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes[J]. **IEEE Transactions on Information Theory**, 2019, 65(8): 4658-4663.

[8] HAO J, XIA S T, SHUM K W, *et al.* Bounds and constructions of locally repairable codes: Parity-check matrix approach[J]. **IEEE Transactions on Information Theory**, 2020, 66(12): 7465-7474.

[9] FU Q, GUO L B, LI R H, *et al.* On the locality of some optimal ternary codes with dimension 6[C]// **2020 13th International Symposium on Computational Intelligence and Design**. Hangzhou, China: IEEE, 2020: 155-158.

[10] CAI H, CHENG M Q, FAN C L, *et al.* Optimal locally repairable systematic codes based on packings[J]. **IEEE Transactions on Communications**, 2019, 67(1): 39-49.

[11] RAWAT A S, PAPAILIOPOULOS D S, DIMAKIS A G, *et al.* Locality and availability in distributed storage[J]. **IEEE Transactions on Information Theory**, 2016, 62(8): 4481-4493.

[12] TAMO I, BARG A. Bounds on locally recoverable codes with multiple recovering sets[C]// **2014 IEEE International Symposium on Information Theory**. Honolulu, USA: IEEE, 2014: 691-695.

[13] WANG A Y, ZHANG Z F, LIN D D. Two classes of (r, t) -locally repairable codes[C]// **2016 IEEE International Symposium on Information Theory**. Barcelona, Spain: IEEE, 2016: 445-449.

[14] HAO J, XIA S T, CHEN B. On the single-parity locally repairable codes with availability[C]// **2016 IEEE/CIC International Conference on Communications in China**. Chengdu, China: IEEE, 2016: 1-4.

[15] BALAJI S B, KUMAR P V. Bounds on the rate and

minimum distance of codes with availability [C] // **2017 IEEE International Symposium on Information Theory**. Aachen, Germany: IEEE, 2017: 3155-3159.

[16] KIM J H, SONG H Y. Hypergraph-based binary locally repairable codes with availability [J]. **IEEE Communications Letters**, 2017, 21(11): 2332-2335.

[17] TAN P, ZHOU Z C, SIDORENKO V, *et al.* Two classes of optimal LRCs with information (r, t) -locality[J]. **Designs, Codes and Cryptography**, 2020, 88(9): 1741-1757.

[18] PRAKASH N, LALITHA V, BALAJI S B, *et al.* Codes with locality for two erasures[J]. **IEEE Transactions on Information Theory**, 2019, 65(12): 7771-7789.

[19] BALAJI S B, PRASANTH K P, KUMAR P V. Binary codes with locality for multiple erasures having short block length [C] // **2016 IEEE International Symposium on Information Theory**. Barcelona, Spain: IEEE, 2016: 655-659.

[20] BAILEY R. Association schemes: Designed experiments, algebra, and combinatorics[M]. Cambridge: Cambridge University Press, 2004.

[21] WANG J, SHEN K Q, LIU X Y, *et al.* Construction of binary locally repairable codes with optimal distance and code rate[J]. **IEEE Communications Letters**, 2021, 25(7): 2109-2113.

[22] WANG A Y, ZHANG Z F, LIU M L. Achieving arbitrary locality and availability in binary codes [C] // **2015 IEEE International Symposium on Information Theory**. Hong Kong, China: IEEE, 2015: 1866-1870.

(本文编辑:孙伟)